AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS:

1. (Currently Amended) An apparatus for detecting adversarial activity on a network, comprising:

a memory configured to store a host table;

a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time;

a translator configured to restore predetermined portions of packet header information of a data packet, the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host, the restoration including to:

extract, from the packet header information, predetermined portions of packet header data including the encrypted host portion of the address,

decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address ~~wherein the predetermined portions include a previously translated address, the previously translated address being extracted from the packet header information, restored into an address from which the previously translated address was translated~~, and

place[[d]] the restored address back into the packet header information of the data packet;

a mapping device configured to map the restored address to the host table;

a host resolution device configured to issue a request to the network to resolve the restored address when the restored address does not match an entry in the host table and to supplement the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid; and

an actuator configured to trigger a security device when the restored address does not match an entry in the host table.

2. (Previously Presented) An apparatus as set forth in Claim 1, wherein the security device is a logging device configured to log the data packet.

3. (Previously Presented) An apparatus as set forth in Claim 1, wherein the security device is configured to signal an alarm when triggered.

4. (Previously Presented) An apparatus as set forth in Claim 1, wherein said host resolution device is configured to derive the host table using an address resolution protocol.

5. (Currently Amended) An apparatus as set forth in Claim 1, further comprising:

a network device configured to place the data packet onto a network when the restored address maps to the host table.

6. (Currently Amended) A method for detecting adversarial activity on a network, comprising:

storing a host table;

repeatedly deriving a cipher key such that the resulting cipher key changes over time;

restoring predetermined portions of packet header information of a data packet, the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host, the restoring including:

extracting, from the packet header information, predetermined portions of packet header data including the encrypted host portion of the address,

decrypting, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address ~~wherein the predetermined portions include a previously translated address, the previously translated address being extracted from the packet header information, restored into an address from which the previously translated address was translated~~, and

placing ~~placed~~ the restored address back into the packet header information of the data packet;

mapping the restored address to the host table;

issuing a request to the network to resolve the restored address when the restored address does not match an entry in the host table and supplementing the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid; and

triggering a security device when the restored address does not match an entry in the host table.

7. (Original) A method as set forth in Claim 6, further comprising:

logging the data packet when the address does not match an entry in the host table.

8. (Original) A method as set forth in Claim 6, further comprising:

signaling an alarm when the security device is triggered.

9. (Previously Presented) A method as set forth in Claim 6, further comprising: deriving the host table using an address resolution protocol.

10. (Currently Amended) A method as set forth in Claim 6, further comprising:

placing the data packet onto a network when the restored address maps to the host table.

11. (Currently Amended) A device for detecting adversarial activity on a network, comprising:

means for storing a host table;

means for repeatedly deriving a cipher key such that the resulting cipher key changes over time;

means for restoring predetermined portions of packet header information of a data packet, the packet header information including a network portion of a destination address routable

over a wide area network and an encrypted host portion of the address identifying a destination host, the means for restoring including:

means for extracting, from the packet header information, predetermined portions of packet header data including the encrypted destination host portion of the address,

means for decrypting, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address ~~wherein the predetermined portions include a previously translated address, the previously translated address being extracted from the packet header information, restored into an address from which the previously translated address was translated~~, and

means for placing ~~placed~~ the restored address back into the packet header information of the data packet;

means for mapping the restored address to the host table;

means for issuing a request to the network to resolve the restored address when the restored address does not match an entry in the host table and supplementing the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid; and

means for triggering a security device when the restored address does not match an entry in the host table.

12. (Currently Amended) A device as set forth in Claim 11, further comprising:

means for logging the data packet when the restored address does not match an entry in the host table.

13. (Original) A device as set forth in Claim 11, further comprising:

means for signaling an alarm when the security device is triggered.

14. (Previously Presented) A device as set forth in Claim 11, further comprising: means for deriving the host table using an address resolution protocol.

15. (Currently Amended) A device as set forth in Claim 11, further comprising:

means for placing the data packet onto a network when the restored address maps to the host table.

16. (Currently Amended) A bastion host comprising at least one computing device adapted for processing packet header information of a data packet, the bastion host being configured to:

store a host table;

repeatedly derive a cipher key such that the resulting cipher key changes over time;

restore predetermined portions of packet header information of a data packet, the packet header information including a network portion of a destination address routable over a wide area network and an encrypted host portion of the address identifying a destination host, the restoring including to:

extract, from the packet header information, predetermined portions of packet header data including the encrypted host portion of the address,

decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address ~~wherein the predetermined portions include a previously translated address, the previously translated address being extracted from the packet header information, restored into an address from which the previously translated address was translated~~, and

place[[d]] the restored address back into the packet header information of the data packet;

map the restored address to the host table;

issuing a request to the network to resolve the restored address when the restored address does not match an entry in the host table and supplement the host table with the restored address upon receipt of a reply to the request that indicates that the restored address is valid; and

trigger a security device when the restored address does not match an entry in the host table.

17. (Currently Amended) The bastion host as set forth in Claim 16, the bastion host being further configured to log the data packet when the restored address does not match an entry in the host table.

18. (Previously Presented) The bastion host as set forth in Claim 16, the bastion host being further configured to signal an alarm when the security device is triggered.

19. (Previously Presented) The bastion host as set forth in Claim 16, the bastion host being further configured to derive the host table using an address resolution protocol.

20. (Currently Amended) The bastion host as set forth in Claim 16, the bastion host being further configured to place the data packet onto a network when the restored address maps to the host table.

21–24. (Cancelled)

25. (Currently Amended) An apparatus as set forth in Claim 1, ~~wherein the address includes a network portion and an apparatus portion,~~ the ~~apparatus~~ host portion of the address having been translated without the network portion also being translated, and wherein said translator is configured to restore the ~~apparatus~~ host portion of the address without also restoring the network portion of the address.

26. (Previously Presented) An apparatus as set forth in Claim 1, wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and

wherein said translator is configured to restore at least a portion of the packet header information in the one or more predetermined fields.

27. (Currently Amended) A method as set forth in Claim 6, ~~wherein the address includes a network portion and an apparatus portion,~~ the ~~apparatus~~ host portion of the address having been translated without the network portion also being translated, and wherein restoring predetermined portions of packet header information includes restoring the ~~apparatus~~ host portion of the address without also restoring the network portion of the address.

28. (Previously Presented) A method as set forth in Claim 6, wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and wherein restoring predetermined portions of packet header information comprises:

restoring at least a portion of the packet header information in the one or more predetermined fields.

29. (Currently Amended) A device as set forth in Claim 11, ~~wherein the address includes a network portion and an apparatus portion,~~ the ~~apparatus~~ host portion of the address having been translated without the network portion also being translated, and wherein said means for translating predetermined portions of packet header information is configured to restore the ~~apparatus~~ host portion of the address without also restore the network portion of the address.

30. (Previously Presented) A device as set forth in Claim 11, wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and wherein said means for restoring predetermined portions of packet header information is configured to restore at least a portion of the packet header information in the one or more predetermined fields.

31. (Currently Amended) A bastion host as set forth in Claim 16, ~~wherein the address includes a network portion and an apparatus portion,~~ the ~~apparatus~~ host portion of the address having been translated without the network portion also being translated, and wherein the bastion host is further configured to restore predetermined portions of packet header information including restoring the ~~apparatus~~ host portion of the address without also restoring the network portion of the address.

32. (Previously Presented) A bastion host as set forth in Claim 16, wherein the data packet includes a translated packet header with a plurality of fields carrying packet header information, the translated packet header including the translated packet header information in one or more predetermined fields of the translated packet header interspersed with un-translated packet header information in fields other than the one or more fields of the translated packet header, and wherein the bastion host is further configured to restore predetermined portions of packet header information including:

restoring at least a portion of the packet header information in the one or more predetermined fields of the header.